How to find hidden cameras

Marc Roessler
marc@tentacle.franken.de

March 25, 2002

"We shall meet in the place where there is no darkness"
– 1984, George Orwell

Abstract

While it was easy to spot cameras twenty years ago due to their large size, this has become increasingly difficult during the last decade. Cameras have become much smaller and consume a fraction of the power they did ten years ago. Due to this, covert installation in nearly any imaginable place is possible. This paper will show methods frequently used for hiding cameras as well as methods to detect and locate covertly installed cameras.

Document available at `http://www.franken.de/users/tentacle/papers/`

1 Introduction

During the last few years the number of surveillance cameras has grown out of bounds. Cameras have been installed in many public and semi-public places such as universities [1], streets, supermarkets, gas stations, parking garages, cinemas, bars, shops, busses, train stations and even discos.

About 25 million CCTV[1] cameras are estimated to be in operation worldwide at the time of writing [2]. Some countries, notably Great Britain, are trying to fully cover every corner of public life with cameras. The Privacy International CCTV page [3] states that between 225 and 450 Million Dollars are spent on surveillance technology in Britain per year, involving an estimated 300.000 cameras. These efforts result in a person driving through the city of London being filmed at least once every five minutes [4]. In the near future cameras may even be installed in all taxis, keeping an eye on the passengers [5]. In Houston, Texas, about 400 cabs have been equipped with such cameras [6].

[1] Closed Circuit Television

It may not be obvious right away why it could be of any importance to anyone to be able to locate hidden cameras. Some will reason that concealed cameras are more or less exotic and thus knowledge on how to find them is not necessary at all. Others even consider interest in how to locate hidden cameras to border the criminal. Both parties err, as shall be illustrated in the following.

Contrary to common belief, hidden cameras are nowhere close to exotic. In 1996 David Fletcher, chief executive of the British Security Industry Association, estimated that employers were spending 12 million british pounds a year on covert camera equipment to monitor their staff [7, p.49]. A survey conducted by the American Management Association found that "33 percent of major U.S. firms say they tape employees – overtly or covertly – to counter theft, violence, or sabotage" [8]. There have been several reports of staff being monitored in changing rooms without their consent [9]. Subminiature cameras were even discovered by the author of this paper during treatment at an oral surgeon's practice: the camera was plastered into the ceiling next to a ceiling light.

Subminiature camera modules are available for as cheap as $ 25 and even ready to use wireless subminiature cameras can be legally bought. Ease of use and the dropping prices highly contributed to the popularity of subminiature cameras. In effect highly miniaturized cameras can be bought, installed and operated even by the average citizen lacking financial resources and technical expertise. Due to this it is not uncommon for subminiature cameras to turn up in places that are in fact neither public nor semi-public. There is a growing number of reports of covert cameras spying on unsuspecting persons in showers, bedrooms and changing rooms [11]. Knowing how to find covert cameras makes the voyeur's job harder. Often even legally installed and operated CCTV cameras are abused to peep on women for voyeuristic purposes. An analysis showed that 15 percent of all targeted CCTV surveillances on women initiated by the camera operator were for "apparently voyeuristic reasons" [7, p.129].

While there is concern that persons interested in finding hidden cameras may have criminal intentions, there are legitimate reasons for such interest as well. One important reason can be concern about privacy and personal freedom. Especially the growing use of face recogniton software [12, 13, 14, 15, 16] is being strongly criticized [17]. There is no way to distinguish cameras that are connected to face recognition systems from those that are not. This is why persons who consider face recognition to touch their personal freedom may choose to avoid surveillance cameras altogether. For instance, they may decide to avoid stores that excessively use video cameras and visit stores that do use significantly less or even none at all. This is not possible unless the presence of cameras is detected in the first place. In countries with lenient privacy protection laws video sequences captured by CCTV cameras may even be legally shown on TV [18], no matter how humilating this may be for the affected persons (for an example see [19]).

Some people might argue that cameras are easy to find and this paper is therefore unnecessary. Be assured that searching for covert cameras is in no way trivial. A modern camera including transmitter and batteries will easily fit inside a box of cigarettes. The Institute of Microtechnology of the University of Neuchâtel (Switzerland) is de-

signing CMOS based subminiature cameras small enough to fit inside a pen [20]. The US company Given® Imaging has even developed an “Ingestible Imaging Capsule” for medical applications that is small enough to be swallowed. The capsule contains a color camera, batteries and a transmitter [21]. Given the size of those cameras it should be clear by now why naive attempts to find cameras will not yield reliable results.

2 Types of cameras and lenses

The focus of this paper will be on electronic cameras. Subminiature photographic cameras exist as well, but those are not as popular as electronic cameras. This is because electronic cameras are more flexible to install and operate. They facilitate real time analysis and can be installed in places that are not easily accessible, since there is no need for changing films. On the other hand photographic cameras provide images far superior in quality to those of standard subminiature video cameras.

Ancient electronic cameras used camera tubes [22, 23] to convert the virtual image of the filmed object to an electronic signal. There are several tube designs [24] which all suffer from drawbacks such as high power consumption, sensitivity to mechanical stress, large size, short lifetime of the picture tube or high lag. Although there are still many tube based surveillance cameras in operation, they are of low importance concerning covert surveillance. Therefore this paper will focus on modern semiconductor based cameras.

The camera does not need to be in the same room as the object under surveillance. It is possible to connect the primary lens to the camera by means of fibre optics [25], which are very similar to those used for medical applications. One advantage of this approach is that very little space is needed where the lens is to be installed. Another advantage is that detection of the lens can be made more difficult by using lens assemblies made of non conductive materials. Lenses prepared this way can not be detected with metal detectors. Still another advantage is that otherwise inaccessible rooms can be surveilled by feeding the fibre cable through sewage or air condition ducts.

Fig. 1 shows some ways to obscure the camera’s lens. Lenses obscured as nail, screw, or rivet head can be seen. Alternatively the lens may be masked as a shirt button (not shown).

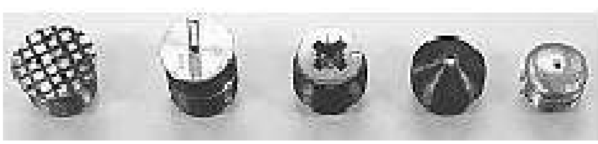


Fig. 1: Obscuring the camera’s lens (Picture courtesy of www.alarm.de)

2.1 CCD cameras

CCD[2] cameras are much smaller than tube based cameras and consume far less power, typically two to five Watts [26]. Particularly interesting for covert surveillance are subminiature CCD board cameras. Subminiature here means something like 32 mm square and 10 mm depth including lens and electronics. A ”board camera” is a camera fully contained on a single circuit board including camera optics and all the electronics needed for generating the standardized video signal.

CCD cameras are available as monochrome (i.e. black and white) and (more expensive) color versions. Several lenses are available such as tele (“zoom”), fisheye (wide viewing angle) and pinhole. Pinhole lenses are small diameter fisheye lenses of typically 2 mm or less in diameter. Pinhole lens cameras are particularly interesting for concealed surveillance applications because they can film through very small holes[3] and even through light-weaved cotton. Monochrome cameras usually are more light sensitive (0.5 to 2 Lux) than their color counterparts (about 3 Lux). A pinhole black and white CCD board camera can bee seen in Fig. 2 at the right side.

Historically the major advantage of CCD cameras has been superior picture quality, but CMOS cameras (see below) are catching up rapidly. Compared to CMOS cameras, the CCD camera’s disadvantages are large size, high power consumption and blooming. Blooming means “leakage” of bright pixels to neighbouring pixels. Bright parts of the picture such as light sources facing the camera will look smeared [27]. Another disadvantage is that CCD cameras can only be operated at temperatures below approximately 55 degrees celsius [28]. In addition they have rather low dynamic range compared to CMOS cameras. This means that CCD cameras will fail to record very brightly lit and very dark objects at the same time. Bright parts of the picture will be overexposed while darker areas will only show black [28].

Black and white CCD cameras are sensitive not only to human visible light but also to radiation in the near infrared (IR) spectrum. This can be demonstrated by having the camera “look” into an active IR remote control as used for most TVs and VCRs. IR remote conrols use light with a wavelength of approximately 900 nm. Light of this wavelength is invisible to humans but can be detected by black and white CCD cameras. The IR pulses that are emitted by the remote control can be seen as a flashing light on the video monitor. This offers some interesting possibilities. If an artificial source of IR radiation is supplied, monochrome CCD cameras can be used without any human visible light source. In effect such cameras can film in “complete darkness”. The mentioned IR emitter can comprise several IR-LEDs[4] grouped together, for example. Another possibility is to use a modified halogen floodlight with an IR pass filter applied to it. In some multiplex movie theatres there are CCD cameras and IR floodlights mounted at the ceiling above the screen, facing the audience. This enables personnel to take a look at what the audience is doing even in complete “darkness”. Color cameras are sensitve to IR radiation as well, but in practice IR sensitivity is too low to be of any use.

[2] Charge Coupled Device

[3] In many cases 1 mm is sufficent.

[4] Light Emitting Diode

2.2 CMOS cameras

Another type of camera which has shown up recently in the catalogues of electronics vendors is based on CMOS[5] technology. CMOS cameras were quite rare a few years ago but are now gaining ground with consumer products such as small handheld devices and webcams. They are available as monochrome and color version with several lenses such as pinhole and fisheye to choose from. Subminiature CMOS cameras usually do not come as board cameras but rather as modules packaged in small plastic cases, as can be seen in Fig. 2. They are about half the price of CCD cameras, less sensitive to electrical distortions, may be operated at temperatures ranging from -40 to +120 degrees celsius [28] and consume far less power (20 to 50 mW) than their CCD counterparts [29, 26]. They can be built much smaller than CCD cameras as major parts of the necessary circuitry can be built directly onto the substrate that carries the light sensors. Just like CCD cameras they are sensitive to IR radiation [23]. In addition they have a high dynamic range [28], i.e. very bright objects and very dark objects can be recorded satisfactorily at the same time.

CMOS cameras have disadvantages as well. Because each pixel comes with a piece of circuitry of its own which consumes room and light, CMOS cameras are not as light sensitive as CCD cameras [30]. Another disadvantage is the lower picture quality, as the individual pixels are quite noisy. There are APS (Active Pixel Sensor) CMOS cameras available which attempt to cancel out the noise, but those are more expensive than the standard PPS (Passive Pixel Sensor) cameras [30]. CMOS cameras do have significant advantages over CCD cameras in regard to noise if large pixel arrays (megapixel arrays) are to be built [31].

CMOS imagers are likely to supersede CCD imagers within the next few years, especially on the consumer market. For more detailed comparisons of CMOS and CCD cameras see [32].

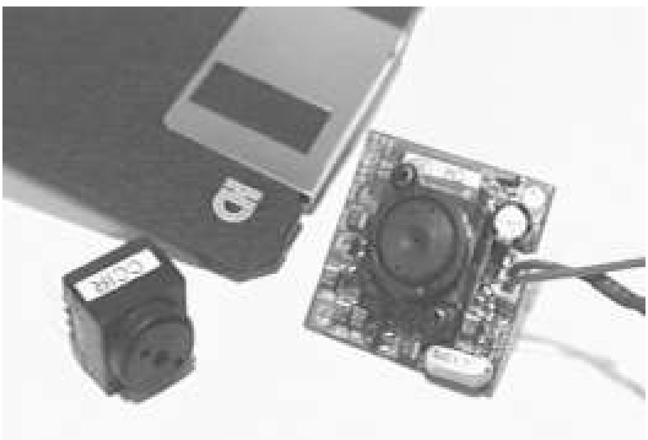


Fig. 2: CMOS (left) and CCD (right) pinhole camera

[5]Complementary Metal Oxide Silicon

2.3 CID cameras

A less frequently used type of camera mentioned for completeness is the CID[6] camera. In contrast to CMOS and CCD cameras the readout of the individual pixels is non-destructive. This makes noise detection and reduction easier [27]. The picture quality is said to be excellent and there is no blooming. CID cameras cover a broad spectrum from near infrared to ultraviolet. The pixels do not have to be read out instantly, thus integration of low light levels over a long time is possible [34, 33]. CID cameras are much more expensive than CCD or CMOS cameras. Up to now they see little use for surveillance applications.

3 Popular hiding places for cameras

There is no single procedure that will reliably detect video surveillance. There are some valuable tools that can help, but their use must always be accompanied by careful visual examination of all potential camera hiding places. Some of the latter as well as frequently used methods for obscuring cameras will be presented below. An important advantage of visual inspection is that it can be conducted on the fly without any pre-planning or tools involved, and of course it is cheapest.

Sometimes it also helps to try to think like someone who wishes to install covert surveillance cameras: Where would *you* hide a camera? At which place would the camera be suspected least?

The following section will present some particularly common or interesting methods and places for hiding cameras. It is by no means a complete list but should suffice to give an idea on what is possible. There are many applications which loosely base on variations or combinations of the presented techniques.

3.1 Distant and off-scene cameras

Some methods to hide cameras solely rely on the way human perception works. A very simple way to “hide” a camera is to install it at a large distance from the space to be surveilled. This does not restrict the usefulness of the camera images in any way because tele lenses can be used to compensate for the distance. For this application there is no need for subminiature cameras, although these are even easier to hide. Standard surveillance cameras painted the right color are very hard to spot and usually have a C-Mount or CS-Mount[7] socket which is needed for attaching the necessary high quality tele lens.

In theory it is very easy to find those cameras as they are not hidden in the original sense. In practice however finding them can prove to be difficult as the camera is hard

[6] Charge Injection Device

[7] Industry standards for mounting lenses

to spot within the large surrounding scenery. This is why there has been disagreement on whether such cameras are to be considered hidden (e.g. [36]). Examples include cameras installed on roofs, church bell towers or trees. Model planes (such as the "MLB Bat" [35]) that are equipped with miniature cameras and transmitters fall in the same category.

Another scheme that is based on how human perception works exploits the fact that cameras usually are expected to be installed at face level or above. Examples for this are cameras installed at service counters below waistline or even at floor level. In most cases those cameras are noticed only by persons that suspect a hidden camera.

3.2 Two-way mirrors

One of the most widely known places for hiding cameras is behind two-way mirrors. Those are frequently seen on TV shows such as "Hidden Camera". Other names for two-way mirrors are "one-way mirrors", "partially silvered mirrors" and "half-silvered mirrors".

Two-way mirrors differ from standard mirrors in two aspects. First they lack the intransparent coating which is applied to the back side of standard mirrors [37]. Second the reflective coating (silver or aluminium [38, 39]) is less dense than that of usual mirrors. The density of the reflective layer can be chosen as desired during manufacturing. The more dense the layer, the more light is reflected and the less light is passed through the mirror.

Because not all of the light that hits the mirror is reflected, two-way mirrors appear to be darker than usual mirrors. However this should not be relied upon when looking for two-way mirrors. Because the density of the reflective coating can be chosen freely there is no definite value to distinguish two-way mirrors from regular ones. If the attacker wants to make sure the mirror is not suspected to be a two-way mirror he will choose more dense coatings. This will result in a visible loss of picture quality, of course.

Tests with normal mirrors[8] showed that standard black and white CCD board cameras can film through those only in bright sunshine. Even then only very brighly lit objects can be seen.

In general two-way mirrors can be seen through in both directions. Sometimes it is possible to take a look through two-way mirrors "the wrong way" by shielding the surrounding light from the mirror. Whether this works largely depends on the density of the reflective coating and the light levels at the viewer's side of the mirror.

In most cases mirrors are easily spotted once an eye is kept open for them. Due to this it is not difficult to find cameras that are concealed behind mirrors. Of course this assumes that the person looking for cameras is able to closely inspect and unmount the mirrors. Unfortunately in many cases this is not possible, such as with wall mounted

[8] Optical mirrors without backside coating that were salvaged from an old document scanner

mirrors on public ground.

Real life examples of mirrors used to obscure cameras include cameras concealed within the rear view mirrors of cars [40] and cameras hidden behind bathroom mirrors [41].

3.3 Ceiling and surroundings

Another place where cameras can be hidden is on top of suspended ceilings. After a small hole is drilled through one of the ceiling tiles a subminiature pinhole camera can be hidden on top of it. Usually there is enough room on top to mount even standard camcorders. In many cases there is no need for drilling any holes because most ceiling tiles have holes of differing sizes for acoustic and design reasons. If the camera is installed next to a light source it is even more difficult to spot. There have already been numerous reports of hidden cameras that were installed on top of suspended ceilings [8].

Cameras may also film through the gratings of ventilation shafts. Alternatively miniature cameras can be hidden inside ceiling mounted smoke detectors[9]. In fact many surveillance technology companys offer prepared smoke detectors [43]. As Steve Mann pointed out [42] the bad thing about those is that tampering with fire equipment (including smoke detectors) is against the law. This means that smoke detectors that are suspected to contain cameras may *not* be dismounted, disassembled or obstructed.

According to a US patent, cameras even may be disguised as fire sprinkler heads [44]. A cylindrical assembly containing mirrors and lenses is mounted within the sprinkler head and the camera itself is mounted on top of the ceiling. This device gives a view of almost 360 degrees round the sprinkler head. Another quite elaborate method is to hide the camera within a prepared floodlight bulb [45, 46].

3.4 Dome cameras

This type of camera can often be seen at train stations and other public places. A dome camera basically comprises a camera mounted within a semi transparent dome. Usually those domes are suspended from or mounted to the ceiling (see Fig. 3). On a casual glance they are easily mistaken as light sources. They often blend in unobtrusively with their environment which is why some consider them to be hidden cameras.

The dome and its interior is painted black, this makes it more difficult to discover the camera installed inside. The camera films through a transparent spot in the black cover of the dome. Some cameras are fixed within the dome while others can be remotely rotated and panned. So-called “speed domes” achieve rotation speeds of up to 400 degrees per second [29]. Some vendors even claim 600 degrees per second [47].

[9] This was shown quite nicely in the film “Enemy of the State®”

Some dome cameras also have a remotely controlled tele lens. This type of camera will enable the operator to closely examine anything within a radius of a few ten meters.



(a) Standard size dome camera



(b) Miniature dome camera

Fig. 3: Above two typical dome cameras that are often installed at train stations can be seen. The miniature dome camera shown in Fig. 3(b) is easily overlooked but by no means the smallest dome camera available.

3.5 Cameras behind LEDs

LED control lights provide an interesting cover for cameras. Some german banks seem to use this technique for integrating surveillance cameras into their automatic teller machines (ATM). The following description is based solely on close examination. No ATMs were disassembled and no information was gained from internal sources.

In Germany some ATMs have an oval plastic cover right above the CRT. Under the plastic cover three green LEDs can be seen. The left and the right LED are intransparent while the LED located in between is clear. The plastic cover and the LEDs serve no obvious purpose.

When the three LEDs are examined closely it can be observed that the LEDs to the left and to the right are clearly three dimensional objects. The viewing angle changes when looking at them from different sides. In contrast the LED in between does not seem to be a three dimensional object. Independent of direction the LED is observed from it always seems to fully face the viewer. This is an indication for a fisheye lens applied to the top of the LED. The interior may look as shown in Fig. 4 (details may differ).

At the top a fisheye lens can be seen. Under the lens there is a two-way mirror fixed

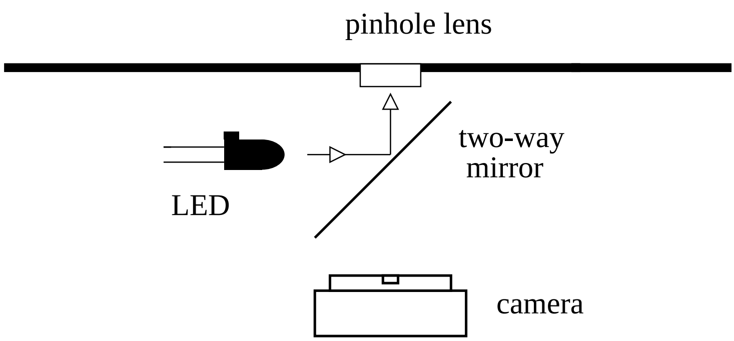


Fig. 4: Camera hidden behind an operating control light

at an angle of 45 degrees. This mirror shields the camera from the view of the customer and reflects the light of the LED to the outside. The reflected light contributes to the covering effect but does not disturb the camera's view.



Fig. 5: LED-Knob

This technique also can be used with any other clear LED controllight. It is advisable to examine power control lights of devices in security critical environments closely.

Fig. 5 shows the headphones volume knob of a CD-Player. The tiny dot at the top of the knob is the butt of a transparent piece of plastic. It guides the light of an LED that is placed behind the assembly through the hollow axis of the knob to the front. It is possible to replace the transparent plastic with an optical system which will transfer the picture to a camera located within the CD-Player. It even may be possible to keep the LED functional by using the technique described before.

3.6 IR pass filters

Another means of obfuscation of camera lenses is the use of infrared (IR) pass filters. Such filters are often used to cover the IR-LEDs of remote controlled consumer appliances such as TVs or VCRs. The filters are intransparent to the human eye but let IR radiation pass almost unaffected. Because monochrome CCD and CMOS cameras are sensitive to IR radiation they can film through IR pass filters. As a result such filters provide a very effective cover for monochrome cameras.

Obviously a source of IR radiation is needed for this to work. In practice this is not a problem. The light emitted by halogen lamps, incandescent lamps and even battery powered flashlights contains enough IR radiation for obtaining pictures of acceptable quality. Matters are more difficult with "cold" light sources such as fluorescent tubes. In this case additional IR emitters need to be installed.

Experiments showed that many semi transparent display covers of CD-Players and VCRs show characteristics very similar to those of IR pass filters. Most display covers let IR radiation pass almost unaffected but prevent the user from examining the internal structure of the display. Cameras installed behind the display covers of household applicances are very difficult to spot.

IR pass filters can also be integrated into wall plates [43]. Similar installations that contain IR pass filters ("black glass" [48]) can often be seen in public restrooms. They house motion sensors that activate water taps, automatic flushing mechanisms or hand driers. Of course nothing prevents anyone from using them as a discrete cover for subminiature cameras.

3.7 Liquid Crystal Displays

Many battery powered digital alarm clocks contain reflective LC Displays (twisted nematic type) [49, 50]. Those LC displays make an almost perfect cover for pinhole cameras.

The following experiment was made with a cheap digital table clock which had an LC display measuring about 5 cm by 3 cm.

The diffusing polarizer foil at the back side of the display was replaced by transparent polarizer foil (see Fig. 6). A hole about two millimeters in diameter was punched through the reflective foil right where one of the digits would be displayed later on. In order to get the pinhole lens close enough to the LC display the circuit board had to be placed outside of the clock. By redesigning the circuit board it would have been possible to make camera and board fit inside the original casing.

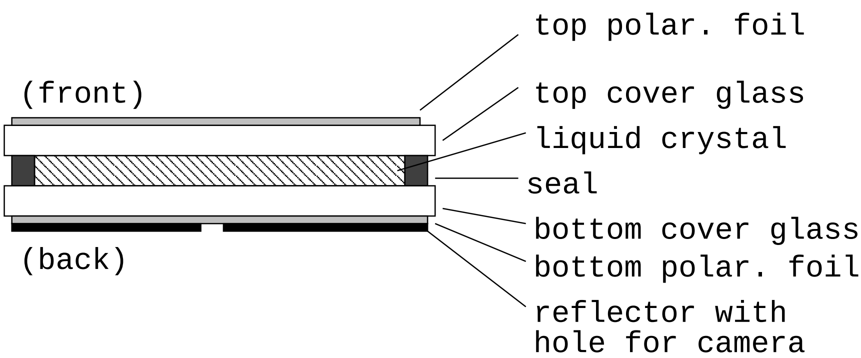


Fig. 6: Modified LC display for use with monochrome CCD or CMOS camera

Active segments of the display cover the hole in the reflective foil surprisingly well. They make the image recorded by the camera fade slightly but this is negligible and does not reduce usefulness in any way. The IR radiation emitted by most light sources passes the dark segments almost unaffected. Unless the clock is examined closely or at a steep viewing angle the hole is not visible at all. Of course this assumes that an

active segment is displayed on top of the hole all the time. This prerequisite can be met by placing the hole beneath one of the dots of the column that separates hours from minutes, for example.

3.8 Outdoor surveillance

Some ways of hiding surveillance cameras outdoors have already been mentioned in section 3.1. Several more will be presented in this section.

There is a US patent that describes how to integrate surveillance cameras into street lamps [51]. The authors of the patent suggest to replace the photo detector on top of the lamp with a small tube that contains a small periscope. In combination with servos this will offer a 360 degree view. The camera can be remotely controlled by means of DTMF audio signals transmitted to the unit via phone lines or other communication channels. As an alternative the camera may be installed inside the lamp housing. In this case it would look downwards through the protective glass cover. The authors further suggest to replace the standard bulb usually used for street lamps with a halogen quartz tube. This may be necessary to free some room for the camera. Because the emitted spectrum of halogen quartz tubes radically differs from that of the standard street lamps[10] color filters must be used, otherwise modified street lamps would be very easy to distinguish from unmodified ones. Another US patent describes how to integrate covert cameras into outdoor lighting fixtures [52].

Among the outdoor installations that can house surveillance cameras are power distribution boxes [53] and power transformers ("pole pigs"). The pole mounted transformers are often seen in the United States and sometimes in Europe as well. For surveillance applications usually dummy transformers are installed which contain only the camera and the necessary communication circuitry. The viewing window of the camera is claimed to be noticeable by taking a close look [51] but of course this should not be relied upon.

Hidden cameras may even be installed in the woods. "Woods Watch" has developed several camouflaged surveillance systems for outdoor use. Cameras hidden within tree stumps, bird houses and rocks are available [54]. The cameras are Hi-8 camcorders with nightshot function and can be activated by passive infrared (PIR) motion detectors and seismic sensors.

3.9 Taking over pre-installed cameras

Another possibility which is rarely thought of is the "takeover" of cameras owned or installed by the victim. This includes cameras that are integrated by default into devices owned by the victim. If the attacker succeeds in gaining control over those cameras, the victim can be spied upon unnoticed.

[10] Usually fluorescent light tubes, sodium vapor lamps or mercury vapor lamps are used.

Though the victim is well aware of the camera she does not consider that it might be used for purposes other than intended by her. In effect cameras that have been taken over are very similar to hidden cameras. Taking over victim owned cameras exploits a common misconception, namely the confusion of the idea of ownership with the idea of control. Owning a device neither makes that device trusted nor does it automatically grant full control over the device.

A good example for cameras that can be taken over are computer controlled miniature cameras, commonly called “webcams”. Those have become very popular recently and are available for prices as low as $ 45. Control over the computer the camera is attached to results in control over the camera itself. Given the fact that trojan based takeovers are trivial with many popular home user operating systems, this is a serious risk. Some trojans even support grabbing images from attached webcams by default [55]. This clearly shows that computer security *does* matter – in many cases a breakin will not only affect the machine itself but also its environment. It is strongly suggested not to attach any microphones or cameras to networked computers permanently. This applys just as well to toys such as the Lego® Mindstorms™ [11] ”Vision Command” set which is essentially a small webcam with added functionality.

Takeover candidates include cameras integrated into hand-helds (PDAs), notebooks (Fig. 7) and cellular phones. The next generation of cellular phones and notebooks will come with builtin cameras by default. A major part of the population will carry at least one device with them that has a builtin camera. Camera takeover attacks can be made highly effective by installing modified firmware. On networked devices such as cellular phones this may be accomplished by means of remote firmware updates. Without doubt this will be exploited by various intelligence services.

Even in the automobile sector there are numerous possibilities for camera takeovers. Some drivers of large vehicles install small board cameras at the rear of the vehicle for easier parking. A paper submitted to the 1998 IEEE International Conference on Intelligent Vehicles even suggests installing CMOS fish eye lens cameras inside cars for making gesture recognition and control of airbags and other devices possible [56]. The authors suggest to mount the camera in front of the rear-view mirror, showing the front part of the car and parts of the rear seats. The authors further suggest to install a second camera in the area of the rear seats for detecting intruders in that area. Another research group developed “Facelab”, an eye-tracking system. The system includes a miniature camera that is installed at the car dashboard and faces the driver. The system will sound an alarm if the driver falls asleep [57, 58].

During the last decade there has been a strong tendency towards video cameras in sensors technology. In the near future PIR (Passive Infrared) motion sensors may be replaced by intelligent video cameras. Video cameras allow a much more fine grained analysis than PIR sensors do [28]. Some prototype computer displays that can display three dimensional objects use video cameras to detect the position of the viewer. This is necessary in order to provide a stable three dimensional display regardless of the angle the screen is viewed at. Other applications such as gesture recognition require

[11] All trademarks are the property of their respective owners. The absence of a trademark sign does not necessarily indicate that the according word or phrase is not a registered trademark.



Fig. 7: CMOS camera built into Sony PCG-C1VE Notebook. The camera can be seen at the top of the screen.

cameras just as well. The needed cameras may be built into the screen or into the keyboard [59, 60].

Even those who do not own any devices that contain cameras are not safe from camera takeovers. CCTV cameras also can be taken over in a number of ways, for example by tapping the video signal cable. Many CCTV camera systems use coax cables, which are easy to tap. Wireless surveillance cameras are even easier to “tap”. In many cases the transmitted video signal is not encrypted and thus can be intercepted easily. Even if the video signal is encrypted it has to be assumed that the encryption can be broken by sophisticated attackers. There are Videoscanners available that scan the channels that are used by most standard 2.4 GHz video links [61]. Mounting that scanner onto a car and driving through the city showed interesting results [62]. In effect this means that the privacy statements of shop owners who install such cameras mean nothing because anyone can receive, analyse, record and publish the transmitted video signal. Wireless unencrypted 2.4 GHz video links were discovered in a fast food restaurant in the city of Berlin, for example.

Some persons believe that surveillance cameras installed in homes for security reasons will be standard in the future [2], “driven by insurance firms and the desire to keep an eye on your property”. The potential for camera takeover is enormous.

3.10 Other hiding places

The list of possible hiding places for cameras can be continued forever. Among the commercially available prepared devices that contain cameras are flower pots, silk plants, bird houses, dolls or stuffed animals [63] (camera may be in the foot [11]), mannequin dolls (camera inside the eye [64]), briefcases, books, folders, pencil sharpeners, pens [67], tissue boxes, shirts, ties, bottles, vitamine bottles, fish tanks, air purifiers and eyeglasses [69].

Among the electronic devices that can contain cameras are portable radios (camera behind the tuning scale), wall clocks, table clocks, radio clocks, wrist watches [65], lamps, coffee machines, emergency lights, exit signs, speakers, VCRs [66], motion detectors [68] and thermostat clocks.

Another interesting method for obscuring the lens is the use of a fake radio antenna. The optics are concealed within the base of the antenna. The light is reflected to the camera by means of several mirrors, similar to a periscope [70]. One of the secrets the suspected russian spy Robert Hanssen is claimed to have exposed is the installation of miniature cameras in the headlights of vehicles of known Russian spies [71]. Similar installations also are suggested by a US patent on “vehicular safety systems” [40].

Often cameras are hidden behind paintings [72] or posters. Prepared paintings and pictures sometimes can be found in the catalogues of electronics mail order supplies.

Cameras be can hidden inside wall mounted light switches quite easily. Many light switches can be modified to contain subminiature CCD or CMOS cameras. Some light switches have small integrated control lights. The covers of those control lights can be used to conceal the camera’s lens. Satisfying results can also be achieved by replacing the cover of the control light with an IR pass filter.

A special application of hidden cameras are body worn cameras. Those may be hidden within a baseball cap and film through holes in the cap. Other possibilities include hiding the camera beneath a shirt or jacket or inside knapsacks or similar body worn items. The lens may be obscured by means of any of the techniques presented in section 2.

4 Electronic aids for finding cameras

Up to this point places for hiding cameras were mentioned as well as techniques which aid in doing so. The information that has been presented so far can give some ideas on what is possible and what to search for. It is a good basis for visual inspection. In most cases, however, visual inspection is not sufficent and must be backed by means of one or several of the techniques presented below. It is advisable to use several of these techniques because this makes detection more reliable in regard to both false positive and false negative alerts. Not all devices and techniques that are mentioned below are easily adopted for home use.

4.1 Metal detector

Though metal detectors originally were not intended to be used as counterespionage tools they can be of use to the counterespionage specialist. Most surveillance devices, including cameras, contain conductive parts that can be detected with a metal detector.

The main problem with metal detectors is that they will detect any conductive object. Because there are a lot of conductive objects in most environments a lot of false alerts will be experienced. This makes reliable detection of surveillance devices very difficult. Depending on the type of metal detector that is used (BFO, pulse or VLF) it is possible to discriminate several metals, but this is of low use in this case. Despite this, metal detectors an still be useful if they are used in combinaton with other tools. In addition they work quite fine for scanning wooden objects such as as desks or cupboards that do not contain any conductors.

Construction plans for simple metal detectors that employ the beat frequency principle (BFO) can be found on the web [73, 74].

4.2 Non-Linear Junction Detector

A device more suited to the application of counterespionage is the so called “Non-Linear Junction Detector” (NLJD). Most electronic surveillance devices contain non-linear components, such as transistors or tunnel diodes. In contrast to metal detectors, NLJDs will only detect non-linear components. Regular conductive objects will not trigger an alert.

The NLJD emits a clean signal in the 900 MHz area and the reflections of this signal are analysed for harmonics. Non-linear components will cause characteristic harmonics to appear within the reflected signal. Those harmonics are not observed in signals reflected by linear components. Non-linear objects can be located at distances of up to a few inches by slowly sweeping suspect areas [75]. NLJDs can even detect unpowered or defective surveillance devices.

They have certain disadvantages as well. Some junctions of different metals show non-linear behavior and thus will result in false alerts. In practice those junctions can be distinguished from electronic parts because they cause a slightly different harmonic pattern. Another method to distinguish the two is to apply mechanical stress to the object under examination. This can be done by hitting it with a rubber hammer, for example. Metallic junctions will change their electronic characteristics and thus modulate the reflected signal, resulting in audible cracks on the receiver. In contrast electronic parts usually keep their characteristics upon mechanical stress and thus will remain silent [76]. It is not known whether it is possible to trick NLJDs by installing certain metallic junctions next to the electronic parts that should be hidden.

An attacker may fool NLJDs by appropriately shielding his surveillance devices. This is possible because NLJDs employ frequencies in the 900 MHz range that can be shielded quite easily [75]. Of course the shield itself is likely to be detected when

scanning for conductive parts, but under some circumstances this technique may be useful to the attacker nevertheless.

It has also been suggested that additional circuitry may be installed that “listens” for strong signals in the frequency bands used by most NLJDs. This circuitry then may destroy itself and the device by means of a high voltage pulse in order to escape detection by the NLJD [75]. It is quite obvious that this may be exploited by the surveillance victim as well, such as by sweeping all objects with a cheap signal generator. 900 MHz cell phones may cause surprising results just as well.

For obvious reasons NLJDs can not be used to detect cameras hidden within other electronic devices. The most important argument against the use of an NLJD probably is its high price.

4.3 Time Domain Reflectometry

In section 3.9 (“camera takeover attempts”) it was suggested that it is possible to take over preinstalled CCTV systems by tapping the cables that carry the video signal. Such taps can be detected by means of a Time Domain Reflectometer (TDR).

TDRs can be used to analyse the reflective properties of wires and cables. The basic principle is to feed pulses of short duration into the cable and view the reflection of the pulses by means of an attached oscilloscope. Splices, taps, short circuits and open ends will cause different behavior concerning reflections and thus can be distinguished from each other [77]. The time between the transmission of the pulse and the reception of its reflection can be read from the oscilloscope screen. Knowledge of this time makes it possible to estimate the distance to the location where the reflection occurs.

Professional TDRs are expensive, but a simple TDR pulse generator can be home made for about $20. In addition to the pulse generator a fast oscilloscope is needed, which can be quite expensive itself. Tomi Engdahl has published plans [78] for a TDR pulse generator based on a circuit idea published in Electronics Design magazine October 1, 1998. He includes some interesting links to additional information on the use of TDRs.

One of the disadvantages of TDRs is that they can not detect capacitively isolated devices and inductive taps [77]. Also after some experiments with the home made TDR it became clear that this kind of analysis does not work well with cables shorter than two or three meters. With short cables the reflection arrived within the so called blind spot [79] and was close to invisible within the rising edge of the pulse. Interpretation of the displayed curves is difficult and requires experience.

4.4 X-ray inspection systems

Counterespionage specialists use X-ray based inspection systems when they suspect that covert surveillance devices were embedded into objects that can not be disassem-

bled easily. As an example, an X-ray scan may be done for detecting bugs that are disguised as standard components (such as a capacitors). Other examples are furniture or devices too costly or precious to disassemble them, such as objects of high personal value or antiques. Similar X-ray scanning system are used for the routine inspection of luggage at airports.

X-ray based inspection systems can be divided into two groups: film based systems and digital systems. Film based systems are the more traditional approach. They are well known to the general public due to their use in the medical sector. With film based systems an X-ray emitter and a sheet of photographic film are placed at opposite sides of the object that is to be examinated. After the film has been chemically processed the typical black and white see-through image can be seen. Because of the high sensitivity of the film only a short pulse of X-rays of sufficent intensity is needed. Digital systems do not use photographic film but an electronic detector. The signals generated by the detector are analysed by a computer which then displays the captured image. The systems that can be seen at airports usually are digital systems.

The major disadvantage of professional X-ray systems is their large size, high weight and high price. Readers who have the necessay budget may consider the site of Heimann Systems [80] (a manufacturer of security related inspection equipment) to be of interest. Skilled readers who do not have the necessary budget might take interest in Jochen Kronjäger's High Voltage and X-ray page [81] which describes the construction of a home made X-ray emitter. Please keep in mind that X-rays pose a major threat to health. It is probably not advisable to use home built devices for detecting hidden cameras. Emission of X-rays in public places is likely to result in legal action and must be considered irresponsible at least.

Most X-ray scanning systems have yet another disadvantage. Usually X-ray sensor and emitter need to be placed at opposite sides of the object under examination. This is not a problem with small objects but will cause trouble if walls or large objects must be inspected. A possible solution to this is a technology developed by the Sandia National Laboratories (Albuquerque, USA) [82]. By carefully analysing the backscattered X-rays it is possible to picture the interior of solid objects. For this technique only one side of the object under examination needs to be accessible. This technology was developed to aid in bomb detection but can be used for other applications just as well. The body scan systems that are used at some US airports use a similar technique [83].

4.5 Detecting video transmitters

In many cases the attacker is unable to install any video cables that conduct the video signal from the camera to his video screen. There are other means of transmission that are far more suited to the attacker's needs than plain video cables, which are time consuming to install. In this section techniques for transmitting video signals as well as techniques to detect such transmissions will be presented.

4.5.1 RF transmission

The classic method to wirelessly transmit signals is to use modulated radio frequency (RF). RF video transmitters can be detected with special equipment such as spectrum analysers. Spectrum analysers graphically display a frequency versus signal strength graph[12]. It is possible to tell from the displayed graph what frequencies a signal is composed of. Video signals have several well known typical characteristics. The standard NTSC color video signal has a bandwidth of 6 MHz (though less than 600 kHz are possible [84]), a line frequency of about 16 kHz and a vertical sync frequency of 60 Hz. Video modulated RF signals thus can be distinguished from other signals.

Analysis can be tricky if the signal is transferred digitally or if frequency hopping, burst transmission or an exotic modulation is used. Examples include the so called spread spectrum technique which masks transmissions as random noise. In this case more sophisticated devices such as Vector Signal Analysers [85] are needed, but this is far beyond the scope of this paper.

In [86] a "video countermeasures device" is proposed that consists of a flashing light bulb. The basic idea is to coerce the camera into generating a video signal of known characteristics. The RF signal emitted by the video transmitter can be identified by scanning the RF bands for signals that match those characteristics.

Standard video links that are available from most HiFi equipment dealers can be detected very easily. Most transmitters operate in the 2.4 GHz band and use one of five freely usable channels. As already mentioned in section 3.9 scanners are available that scan those channels for video signals [61]. Because this type of scanner only scans a fixed set of frequencies it can not be used to reliably detect RF video transmissions.

4.5.2 Wire bound transmission

Wireless transmission is not the only way to transmit video signals without installing any additional cables [84]. The video signal can be transmitted by means of unused power wiring or telephone lines. Even though power wiring is by no means adapted to the impedance of the video signal source it is possible to transmit the signal across some distance. In an experimental setup the video signal was fed into an otherwise unconnected extension cord of 15 meters in length. At the remote end of the extension the video signal still resulted in acceptable picture quality. Though quality can not be expected to meet broadcast standards the signal still is perfectly usable. With a simple amplifier and differential transmission distances of up to 1500 meters can be achieved with twisted pair cable [90], up to 700 meters with telephone wiring [91]. Baseband transmission can be difficult if no unused wire pair is available. In this case the attacker may modulate a carrier with the video signal and feed this signal into the power wiring. This technique is called carrier current transmission and is used by most wire bound babyphones, for example. Both carrier current transmission and baseband

[12] This is can be accomplished with a computer doing Fast Fourier Transformation (FFT) or by means of purely analog circuitry.

transmission can be detected by analysing all conductors with signal analysis tools such as oscilloscopes and spectrum analysers.

Conductors do not necessarily need to be wires. Keep an eye on anything conductive that is not implicitly grounded. Even drain pipes that contain water should be measured. In an experimental setup video signals were successfully transmitted by means of an iron banister that extended across three floors, without using any additional amplifiers.

4.5.3 Optical video links

As an alternative the video signal may be transmitted optically by means of an Infrared (IR) transmitter. This also works with visible light, but this is rarely done because such visible links are easily discovered. The emitter may use a IR semiconductor laser or several IR LEDs grouped together. Optical video links can not be detected by standard RF detection equipment except for the local emissions of the IR transmitter control circuitry.

Because IR radiation can not be detected by the human eye additional tools such as IR sensitive CMOS or CCD cameras are required for detecting IR transmitters. For sharply focused transmitters it can be necessary that the camera faces the transmitter, otherwise smoke must be used as a reflector to render the IR beam visible. Keep in mind that the attacker's receiver needs to face the transmitter, too. Alternatively he may guide the rays by means of mirrors or window panes, but visual contact must always be made somehow. Detailed analysis of any discovered IR radiation is possible with IR sensors coupled to signal analysis tools.

4.5.4 Communication networks

The video signal can also be transferred by means of communication networks. Examples are analog and ISDN phone lines, mobile phone networks and computer networks. Data may be fed into those networks by taking over victim owned cameras that are attached to networked devices (see Section 3.9). Instead of taking control over a networked device that is owned by the victim the attacker may choose to install additional miniature computers the victim is not aware of. Such miniature computers can be small embedded special purpose systems. Examples are special webcam servers that include a tcp/ip stack and an ethernet interface. If IP traffic is considered too obvious, as an alternative the video stream may be transmitted at the ethernet layer. Another example are video stream servers that can be attached to ISDN networks.

The obvious approach for detecting video signals transmitted on regular communication networks is to monitor all networks. This will detect plain video transmissions but will fail to detect video data disguised as innocuous data. As an example, the attacker may make a workstation do a webcam snapshot. The captured image then could be sent one piece a time by replacing the Mail-IDs of all outgoing mail with chunks of base64 encoded picture data. If the attacker can sniff the outgoing traffic somehow he

will be able to combine the data into the complete snapshot. Such transmission paths, commonly known as “covert channels”, are difficult to prevent.

4.6 Detecting the camera’s emissions

Most cameras emit a typical spectrum of electromagnetic noise. The emissions mostly result from the pixel readout clock signal and components of the video signal. The emitted spectrum is quite similar for any camera that generates a standard video signal. It is possible to locate electronic cameras by scanning for this spectrum. Depending on the frequencies of the signal components proper shielding may foil detection attempts, but often cameras are not shielded at all.

4.6.1 Detecting the clock signal

Most CCD board cameras and CMOS module cameras use one out of a small set of well known standard clock frequencies. Table 1 lists some typical values. The OV5016 single chip camera that is mentioned in the table is used in the camera that can be seen in Fig. 2 at the left. The CCD camera shown in Fig. 2 at the right uses the KS7214 timing/sync generator that is listed in Table 1.

Sync Generator or Camera	NTSC/EIA clock	PAL/CCIR clock
CXD2463R, KS7214	19.06992 MHz 28.63636 MHz	18.93750 MHz 28.37500 MHz
OV5116, OV5006 series, V-X0071	12.288 MHz	13.5 MHz
OV7500	14.318181 MHz	17.73265 MHz
VV5430	12.0000 MHz	14.7456 MHz

Table 1: Clock frequencies of some common camera and sync generator chips. CXD2463R and KS7214 are sync generator chips for CCD cameras, all others are single chip CMOS cameras. See references [92] to [98] for further details.

In order to get an idea on what the emitted frequency spectrum looks like the emissions of a CMOS and a CCD camera were measured by means of a magnetic test loop connected to a spectrum analyser. The tested cameras were the two cameras shown in Fig. 2.

Fig. 8 shows the frequency spectrum emitted by the subminiature single chip CMOS camera that is based on the OV5016 chip [97]. According to the OV5016 datasheet [95] this camera uses a clock frequency of 13.5 MHz. The peak of the clock signal shows up very well in the spectrum. Most of the other peaks are harmonics of the clock frequency. Those peaks are located at 26.7 Mhz, 40.0 MHz, 53.4 MHz, 66.7 MHz, 80.1 MHz and 93.6 MHz. For this measurement the camera was set up exactly as suggested by its manual, including 78L05 voltage regulator and filter capaciators. The sudden jump in sensitiviy at 30 MHz is due to an automatic change in bandwidth of the spectrum analyzer.

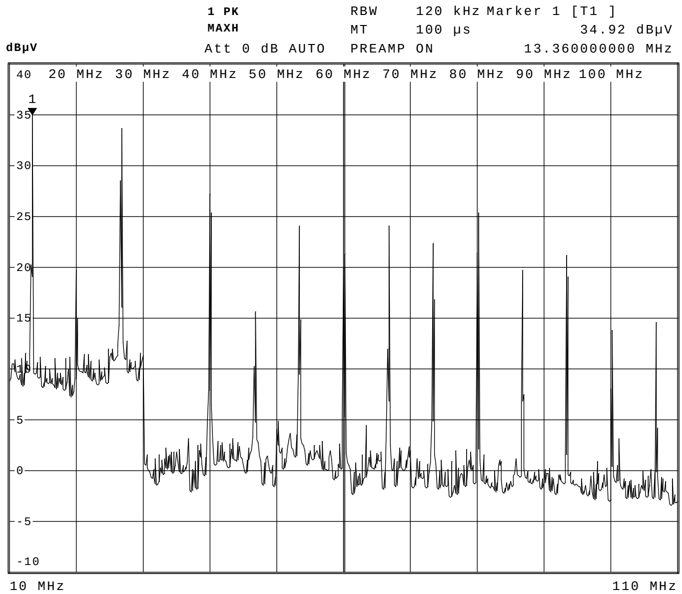


Fig. 8: Emissions of the tested CMOS camera. The clock frequency at 13.6 Mhz and its harmonics at 26.7 MHz, 40.0 MHz, 53.4 MHz, 66.7 MHz, 80.1 MHz and 93.6 MHz can be seen.

Fig. 9 shows the emissions of the tested CCD pinhole camera. The sync and timing generator chip (KS7214) on this camera's board uses a clock frequency of 18.93750 MHz which shows up clearly in the spectrum. Its harmonics are located at 37.9 MHz, 56.8 MHz, 75.8 MHz and 94.7 Mhz. Note that the two diagrams have different scale, the emissions of the CCD camera are much stronger than those of the tested CMOS camera module.

The clock frequencies of most miniature cameras are within the range of the short wave band. Short wave band receivers thus can aid in locating hidden cameras. With a Sony ICF-SW100 multi band receiver the signals of the tested CMOS module board and CCD board cameras could be "heard" at a distance of up to 10 cm and 50 cm, respectively. It is interesting to note that the 20 MHz peak of the CMOS camera could be received up to a distance of 40 cm, despite the fact that the emissions at 13.6 Mhz are much stronger, according to the spectrum analyser graph. With more sensitive equipment that does not rely on audible signal modulations it is possible to detect the clock signal at much larger distances.

The received clock signals can be distinguished from other random signals quite easily. It was found that the clock signal that is emitted by the camera is amplitude modulated with parts of the video signal. When the demodulated audio signal that the shortwave band receiver generates is displayed with an oscilloscope the vertical sync pulses can be seen. With the tested CCD camera it was even possible to estimate the distribution of luminance across the picture based on the displayed wave form. Partly

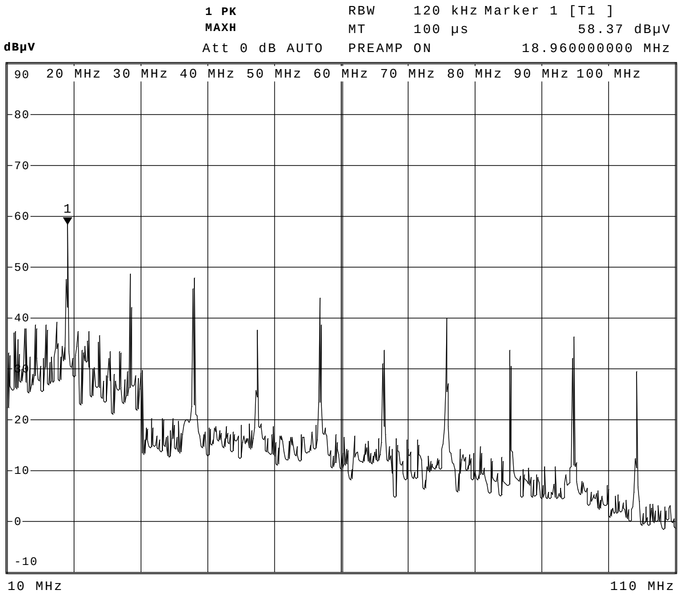


Fig. 9: Emissions of the tested CCD camera. Note the clock frequency peak at 18.96 Mhz and its harmonics at 37.9 MHz, 56.8 MHz, 75.8 MHz and 94.7 Mhz.

covering the camera or changing the light levels in the room resulted in clearly visible changes in the displayed waveform.

As expected shielding reduced the emissions to almost zero. Another disadvantage of this method for locating cameras is that the weak clock signal is easily missed in electrically noisy environments such as computer rooms. Even digitally controlled HiFi equipment can cause significant interference.

4.6.2 Detecting the line frequency signal

An important component of any video signal spectrum is the line frequency. The line frequency specifies at which intervals the horizontal sync pulse occurs. With standard video signals the line frequency is roughly 16 kHz. The exact value is 15.625 kHz for CCIR/PAL video signals and 15.750 kHz for EIA/NTSC video signals [29]. It is emitted at low strength by video cables and video cameras. Insufficently shielded cameras and can be detected by means of VLF (Very Low Frequency) receivers [87]. One author claims that similar receivers were used by the german “Post” for locating unlicensed TVs [89]. Simple consumer grade VLF receivers are available at some spy gadget shops. They are easy to use but quite expensive and not very flexible.

Basic VLF receivers are simple in design. The schematics for the VLF receiver that was used for the following experiments can be found in Appendix A. For signal analy-

sis a 44 kHz PC soundcard[13] and spectrum analyser software was used. Depending on the distance between the camera and the VLF antenna a peak at the line frequency can be observed on the displayed spectrum graph.

Several pickup coils were tried as antennas. Tests with a simple 2 cm coil showed promising results. The distance at which cameras could be detected was increased almost by four times by using a resonant coil wound on a ferrite rod. Details on the construction of this coil can be found in Appendix B.

Table 2 lists the distances at which various devices could be detected. As a pickup coil the resonant ferrite coil was used. The distances are conservative values – at the listed distances the 16 kHz peak could be identified without any doubt left. Small peaks that may be interpreted as line frequency components could be noticed at even larger distances. Also consider that the pickup coil is a non-optimized experimental version. With professional equipment it is possible to detect cameras at greater distances [84].

Camcorder	90 cm
Camcorder, shielded (one layer 0.015 mm Al foil)	70 cm
Camcorder, shielded (two layers 0.015 mm Al foil)	55 cm
CCD board camera	8 cm
CCD board camera, shielded (one layer Al foil)	6 cm
CCD board camera power cable (unshielded 15 cm cable)	10 cm
CCD board camera video cable	10 cm
CMOS camera module	3 cm
video signal on cable RG-58U (50 Ω)	–
video signal on 75 Ω cable	–

Table 2: Detection distances of various cameras

Table 2 shows that shielding can have some effect if it is done properly. There are significant differences concerning the emissions that are caused by the video cables. With the RG-58U and the 75 Ω video cables no emissions could be measured at all. In contrast the small diameter video cable that came with the board camera caused much stronger emissions than the camera itself. The unshielded DC power supply cables emitted signals of comparable strength. The signal emitted by the tested CMOS camera module probably is too weak to be detected in real life situations.

VLF receivers do not detect cameras, they detect the video signal that is generated by the cameras. In effect VLF receivers will detect TVs and improperly shielded cables that carry video signals, too. This can be considered both an advantage and a disadvantage. The advantage is that a VLF scan can not only detect the cameras themselves but also cables that are used by the attacker. This is especially useful in cases where the attacker uses preinstalled unshielded cables such as telephone lines for conducting the video signal to the outside (see section 4.5). The VLF receiver's ability to locate video cables and TVs may be considered a disadvantage if such have been installed legitimately, such as with CCTV systems.

[13] Sampling rates lower than 44 kHz are not recommended.

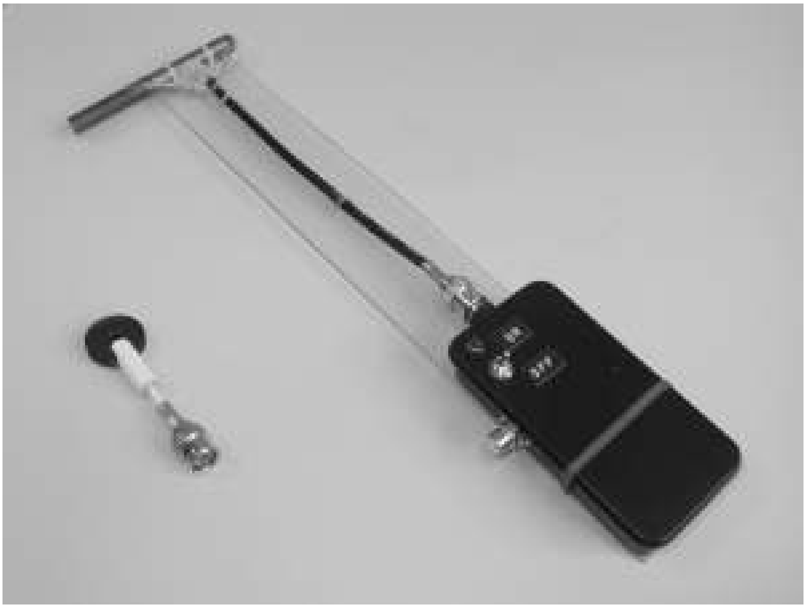


Fig. 10: VLF receiver with resonant ferrite coil. Due to the BNC connectors the coils can be changed easily. Lefthand a simple non-resonant pickup coil can be seen.

Another disadvantage is that the presented VLF receiver can not reliably detect cameras that use line frequencies other than 16 kHz or even no fixed line frequency at all. Examples for such cameras include webcams. There are two possibilities to get around this. One is to measure all commonly available video capture devices for typical emissions and then scan suspect areas for those emissions. Another possibility is to watch the whole low frequency spectrum for suspicious peaks. Both methods are not very practical. They exclude the use of resonant pickup coils as well, because those only attenuate fixed frequencies. Nevertheless the presented VLF receiver can be a valuable tool when scanning for hidden off-the-shelf cameras.

4.7 Detecting thermal emissions

Most electronic devices have at least one thing in common: they heat up because of losses along conductors. After some time the device will have warmed up enough to emit a thermal spectrum that can be detected by suited thermal imagers [99]. This is especially useful for CCD cameras as those have a high power consumption and therefore high thermal losses.

Murray Associates proposes a technique called Thermal Emissions Spectrum Analysis® (TESA®) [100]. They use a sensitive thermal imager that can detect thermal differences as low as 0.1 degrees celsius. The TESA camera looks similar to a regular video camera. The difference is that the thermal imager will display objects that radiate thermal energy as bright spots. In contrast to the techniques that rely on various

electronic emissions this technique is not easily fooled if the camera is switched off as soon as a bug sweep is suspected. This is because the camera and the surrounding matter will keep its raised temperature long enough to be detected by TESA scans.

A major disadvantage of this technique is that cameras installed right next to or inside light sources will most likely not be detected within the "thermal blaze". It is unknown whether TESA will detect low power CMOS cameras. CMOS cameras generate only a fraction of the heat CCD cams do and thus may be more difficult to detect. Murray Associates claims that their TESA scan can even reveal activated microphones by showing thermal differences, so CMOS cameras may show up as well.

4.8 Detection by means of a Laser

Science&Engineering Associates (SEA Inc.) has developed a product named "SpyFinder™". It employs two low power (below 5 mW/Laser Class III) lasers with a wavelength of about 635 nm (visible red spectrum) [101, 102, 87]. It works optically using "proprietary optics". The camera is said to appear as a blinking red light in the viewing window. This is claimed to work against all kinds of cameras even when unpowered, within a distance of 5 to 50 feet. The device is further claimed to detect night vision devices (at distances of up to more than 50 meters) and binoculars [87]. A consumer grade version of this device also is available [103].

The quoted texts do not make it clear how the device works. One text states that the consumer grade version employs an "invisible detection beam", and that the "camera's lens reflects back as a flashing dot in the SpyFinder's viewer" [104]. Kevin D. Murray from Murray Associates notes that neither the commercial version nor the consumer grade version can detect cameras that are hidden behind an IR filter [88]. Judging from the facts presented a vague guess is that the device detects reflective circular curved objects (which a lens usually is).

5 Conclusion

Several locations and techniques that are frequently used for hiding subminiature cameras were presented. In addition technical countermeasures were described. Though this document does not make the reader a counterespionage specialist, it provides some basic information which can be used to detect simple espionage attempts. Feedback on cameras that were detected by using the information presented within this paper is welcome.

Keep in mind that the first step towards finding hidden cameras is suspicion. Contrary to popular belief hidden cameras are *not* rare. There is no easier target for a would-be voyeur than a non-suspecting person. Do not panic but be aware of the potential threat. Without doubt cameras will become still smaller during the next decade and thus even more difficult to locate. The "Smart Dust" project of the University of California, Berkeley might give an idea of what is yet to come [106].

Acknowledgement

I would like to thank the following persons for their reviews, comments, support and contributions:

Basti, Matthias Brüstle, Robert Dorn, Florian Grüner, Renato Romero, Roland Schulz and Prof. Dr.-Ing. M. Albach and Dr.-Ing. H. Rossmanith from University of Erlangen.

Appendix A Construction of a VLF receiver

A simple VLF receiver can be built from only a few components. The design centers around an operational amplifier. The circuit shown in Fig. 11 is based on designs published by R. Romero [105].

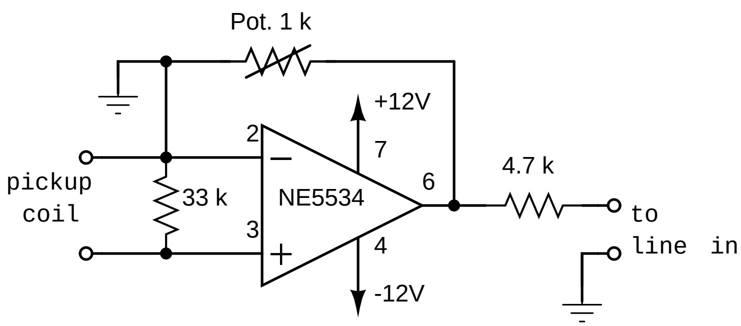


Fig. 11: VLF receiver circuit

As operational amplifier the high performance low noise type NE 5534 from Philips can be used. Even better results can be achieved with the op-amp OP-27. Two batteries are needed for providing the symmetric power supply. Two 9 V batteries suffice as ± 9 V is well within the range of ± 3 to ± 20 V which the data sheet of the NE 5534 specifies. It is advisable to buffer the supply voltage with two electrolytic capacitors of 10 μF each. Keep in mind that the signal output has a significant DC component. Nearly 5 V DC were measured at the output of the built test circuit. Decoupling by means of a capacitor with a value of a few μF is possible but will slightly degrade the signal and cause potentially unwanted attenuation of certain frequencies.

Take care not to apply any strong pulses or signals to the coil such as by placing it near power transformers or by moving strong magnets around near it. This will saturate the operational amplifier and may even cause permanent damage. Do not apply power to the VLF receiver unless the pickup coil is installed, otherwise the op-amp may start oscillating. All signal cables must be shielded and the amplifier circuit should be built into a conductive casing. Keep in mind that touching the pickup coil can result in reception of AM radio stations. Make sure that the unit can be moved around easily for

scanning without the need to touch any part of the pickup coil.

The generated audio signal is roughly line-in level, i.e. it can be fed to line-in connectors of HiFi components or soundcards of personal computers.

Appendix B Construction of a resonant ferrite coil

The resonant pickup coil consists of a capacitor connected in parallel to an enamel copper wire coil that is wound on a ferrite rod. Thus a tank circuit is formed which will resonate at a certain frequency dertermined by Thomson's formula:

$$f_{res} = \frac{1}{2\pi\sqrt{L \cdot C}}$$

The inductance L and the capacity C must be matched to resonate at the desired frequency of roughly 16 kHz. In most cases L will be unknown, so the easiest solution is to start with a capacity of roughly 47 nF and a ferrite rod fully wound with enamel copper wire. The process of tuning the tank circuit is done by repeatedly determining the resonant frequency and removing windings of the coil as needed.

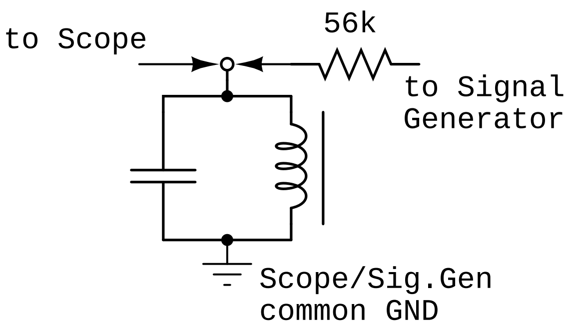


Fig. 12: Setup used for determining the resonant frequency

The resonant frequency of the tank circuit can be determined by using a tunable sinus generator and an oscilloscope. Use of the setup presented in Fig. 12 is suggested. Tune the signal generator to the frequency that results in maximum signal amplitude on the scope screen. This frequency is the resonant frequency. For most resonant coils it is not important to hit the line frequency exactly because the frequency response of the coil is still quite flat, i.e. it has no sharply defined resonant frequency.

The coil that was used for the presented experiments consists of 0.2 mm enamel copper wire wound on a ferrite rod 9 mm of in diameter and 10 cm in length. A capacitor with a value of 47 nF was used.

References

[1] Corinna Schöps, Uni-SPIEGEL, June 2001: Im Haus der 1000 Augen

[2] Jane Wakefield, BBC News, February 7, 2002: Watching your every move
`http://news.bbc.co.uk/hi/english/sci/tech/newsid_1789000/1789157.stm`

[3] Privacy International's page on Closed Circuit TV (CCTV)
`http://www.privacyinternational.org/issues/cctv/`

[4] Detlef Borchers/pab, c't 24/2000: Videoüberwachung mit begrenztem Nutzen

[5] mediaeater Taxi Cab Notes 4.23.2000 v1.b: Taxi & Limousine Commission (New York, NY, USA) March 2000 Press Release (Industry Notice #00-08): TLC authorizes in-vehicle digital camera as alternative security device to satisfy FHV partition requirement
`http://www.mediaeater.com/cameras/news/taxi.html`

[6] Cabbie Cams Hit The Road: Pilot Program Tests Digital Cameras In NYC Taxis
`http://www.governmentvideo.com/issues/2000/0100/stories/0100.security.shtml`

[7] CLIVE NORRIS. GARY ARMSTRONG. *The Maximum Surveillance Society – The Rise of CCTV.* Berg, 1999.

[8] Dana Hawkins, U.S.News, January 17, 2000: Cheap video cameras are monitoring our every move
`http://www.usnews.com/usnews/nycu/tech/articles/000117/nycu/watch.htm`

[9] Lyn Nell Hancock, Claudia Kalb and William Underhill, Newsweek, July 17, 1995: You Don't Have to Smile
scan available at `http://wearcam.org/newsweek_sheraton_locker_rooms.gif`

[10] Bill Lubinger, Newhouse News Service, March 12, 2001: Home, Snoop Home: Spy Camera Becoming Just Another Appliance
`http://www.newhouse.com/archive/story1a031201.html`

[11] Mark Boal, The Village Voice, Sept 30 - Oct 6, 1998: The Surveillance Society, Part One: Spycam City
`http://www.villagevoice.com/issues/9840/boal.shtml`

[12] Chris Nuttall, BBC News, Tuesday, October 27, 1998: Watching Big Brother
`http://news.bbc.co.uk/hi/english/sci/tech/newsid_202000/202024.stm`

[13] BBC News, Tuesday, October 13, 1998: Candid camera for criminals
`http://news.bbc.co.uk/hi/english/uk/newsid_191000/191692.stm`

[14] Mark Arner, The San Diego Union-Tribune, November 11, 2000: Convention for chiefs of police displays crime-fighting tools
Available from the Union-Tribune archives at `http://pqasb.pqarchiver.com/sandiego/`

[15] CNN, July 2, 2001: Tampa uses cameras to scan for wanted faces
`http://www.cnn.com/2001/TECH/ptech/07/02/high.tech.security.ap/`

[16] Thomas C Greene, The Register August 13, 2001: Think tank urges face-scanning of the masses
`http://www.theregister.co.uk/content/6/20966.html`

[17] Philip E. Agre: Your Face Is Not a Bar Code – Arguments Against Automatic Face Recognition in Public Places
`http://dlis.gseis.ucla.edu/people/pagre/bar-code.html`

[18] Mark Boal, The Village Voice, Dec 2-8, 1998: The Surveillance Society, Part Two: Spycam Chic
`http://www.villagevoice.com/issues/9849/boal.php`

[19] Tessa Mayes, Spiked June 27, 2001: No privacy in public?
`http://www.spiked-online.com/Articles/00000002D150.htm`

[20] Institute of Microtechnology of the University of Neuchâtel, Switzerland: CMOS-based "Miniaturized low-power camera system"
`http://www-imt.unine.ch/ESPLAB/www/projects/Microcam/`

[21] Given Imaging (Ingestible Imaging Capsule)
`http://www.givenimaging.com`

[22] PETER ZASTROW. *Fernsehempfangstechnik*. Frankfurter Fachverlag, 1987.

[23] Al Colombo: CCTV - Video Surveillance Cameras - Monitors - Security Monitoring Devices
`http://www.infosyssec.org/infosyssec/cctv_.htm`

[24] North American Imaging, Inc: Camera Tube Descriptions
`http://www.tubenet.com/camera.html`

[25] MK Photonics "FiberSpy"
`http://www.fiberspy.com`

[26] CMOS vs. CCD
`http://www.switkin.com/software/meng/cmosvsccd.html`

[27] Choosing imaging sensors for visible light (CCD, CMOS, CID)
`http://www.industrialtechnology.co.uk/1999/jan/siraimaging.html`

[28] José Emilio Santos Conde: *Optische Raumüberwachung*. Dissertation Universität Duisburg 2001
`http://www.ub.uni-duisburg.de/diss/diss0119/santosdiss.pdf`

[29] MICHAEL GWOZDEK. *Lexikon der Videoüberwachungstechnik*. Hüthig, 1997.

[30] CCD and CMOS image sensors
`http://www.photocourse.com/01/01-04.htm`

[31] L.J. Kozlowski, J. Luo, A. Tomasini. *Performance Limits in Visible and Infrared Imager Sensors*. IEDM 1999, Tech. Digest, IEEE (1999)

[32] STUART A. TAYLOR. CCD and CMOS Imaging Array Technologies: Technology Review. Technical Report EPC-1998-106
`http://www.xrce.xerox.com/publis/cam-trs/pdf/1998/epc-1998-106.pdf`

[33] Chester F. Carlson Center for Imaging Science: CID an Overview
`http://www.cis.rit.edu/research/CID/overview.htm`

[34] What is a CID
`http://www.cis.rit.edu/research/CID/a_cid_is.htm`

[35] MLB Bat – a small aircraft including camera and transmitter used as a video platform
`http://www.spyplanes.com`

[36] comp.society.privacy Computer Privacy Digest Volume 5, Issue 7: Video Camera on Utility Poles
`ftp://ftp.cs.uwm.edu/pub/comp-privacy/volume5/V5%23007`

[37] HowStuffWorks: How do one-way mirrors work?
`http://www.howstuffworks.com/question421.htm`

[38] Cambridge Technology mirrors
`http://www.camtech.com/mirrors/mirrors.htm`

[39] Gemini Observatory factsheet on mirror coatings
`http://www.gemini.edu/media/factsheets/coatingfacts.html`

[40] United States Patent No. 6,151,065. Nov 21, 2000. Van P. Steed, Scott J. Arnold, Robert K. Cejka. *Concealed Integrated Vehicular Camera Safety System*

[41] Vernon Silver, In Formation magzine: Jeeper Peepers – Invasion of privates
`http://www.informationmag.com/jeepers.html`

[42] Steve Mann: Surveillance cameras versus wearable cameras: smoke detector cameras
`http://wearcam.org/camera_taxonomy.html`

[43] United States Patent No. 6,064,430. May 16, 2000. Stephen Lefkowitz. *Discrete Surveillance Camera Devices*

[44] United States Patent No. 4,963,962. Oct. 16, 1990. Kruegle et al. *Optical Surveillance Assembly and Camera*

[45] Supercircuits: camera obscured as a floodlight bulb
`http://www.supercircuits.com`

[46] Wireless Floodlight Camera
`http://www.smarthome.com/7528.html`

[47] Iteris DC-100 Outdoor Dome Camera data sheet
`http://www.iteris.com/html/products/pimages/dc100.pdf`

[48] Steve Mann: Privacy issues of wearable cameras versus surveillance cameras
`http://wearcam.org/netcam_privacy_issues.html`

[49] IBM: About reflective LCD
`http://www.trl.ibm.co.jp/projects/reflcd/ref_expe.htm`

[50] University of Dayton Computer Science Department: Display Technologies
`http://www.udayton.edu/~cps/cps460/notes/displays/`

[51] United States Patent No. 5,886,738. Mar. 23, 1999. Hollenbeck et al. *Apparatus within a Street Lamp for Remote Surveillance*

[52] United States Patent No. 6,259,476. July 10, 2001. Kenneth L. Greene. *Lighting fixutre with a covert security camera*

[53] Outdoor camera hidden within a power distribution box
`http://www.electron.de`

[54] Woods Watch Custom Camouflaged Surveillance Systems
`http://www.woodswatch.com`

[55] The Cult of the Dead Cow's Bo2k, a "network administration tool"
`http://www.bo2k.com`

[56] S.-B. Park, A. Teuner, B. J. Hosticka and G. Triftshäuser: *An Interior Compartment Protection System Based On Motion DetectionUsing CMOS Imagers.* 1998 IEEE International Conference on Intelligent Vehicles
`http://www.daimlerbenz.com/research/events/pdf/IV980164.PDF`

[57] Sleepy drivers to be saved by dashboard spy
`http://www.ananova.com/news/story/sm_249975.html`

[58] GlobalTechnoScan: Asleep at the wheel
`http://www.globaltechnoscan.com/28thMar-3rdApr01/asleep.htm`

[59] Ulrike Kuhlmann, c't 25/2001: Über den Tellerrand – Räumliche Darstellung auf Flachdisplays

[60] Dialog-based Human-Technology Interaction by Coordinated Analysis and Generation of Multiple Modalities
http://smartkom.dfki.de

[61] Bogerfunk electronics Video scanner
http://www.boger.de/video_e.htm

[62] Radio-Scanner 4/99: Werkzeug gegen Videowanzen

[63] Hidden Camera products
http://www.hiddencamera.com

[64] United States Patent No. 4,982,281. Jun. 1, 1991. Frederic J. Gutierrez. *Surveillance System having a Miniature Television Camera mounted behind an Eyeball of a Mannequin*

[65] CCD camera integrated into wrist watch
http://www.x20.org/spygear/

[66] Hidden Camera Solutions
http://www.concealedcameras.com

[67] Camera conealed as a pen
http://www.spycameras.net/body_worn.htm

[68] Cameras inside tissue boxes and motion detectors
http://www.hiddenpinholecameras.com/hiddencameras.htm

[69] Sunglasses camera
http://www.pimall.com/nais/v.eyeglass.html

[70] United States Patent No. 5,495,370. Feb. 27, 1996. John Tuffen. *Surveillance Devices*

[71] Pierre Thomas, ABCNews March 24, 2001: America's Cutting-Edge Espionage Techniques at Risk
http://more.abcnews.go.com/sections/us/dailynews/spy_thomas.html

[72] The Urban Monitor: Spot the hidden camera.
http://www.mongrelmedia.co.uk/unknownpages/hiddencamera.htm

[73] Build your own metal detector
http://home.clara.net/saxons/diy.htm

[74] Metal Detector Construction Plans
http://www.geocities.com/Paris/Musee/3308/md_plans.html

[75] Granite Island Group: Technical Surveillance Counter Measures. Non Linear Junction Detector Review and Tutorial
`http://www.tscm.com/tmdenljd.html`

[76] Ralph D. Thomas: Understanding Non-Linear Junction Detection
`http://www.pimall.com/nais/n.junction.html`

[77] Granite Island Group: Technical Surveillance Counter Measures. Time Domain Reflectometry Analysis
`http://www.tscm.com/tdr.html`

[78] Tomi Engdahl's TDR plans
`http://www.hut.fi/Misc/Electronics/circuits/tdr.html`

[79] Granite Island Group: Technical Surveillance Counter Measures. TDR Tutorial - Introduction to Time Domain Reflectometry
`http://www.tscm.com/riprcop.html`

[80] Heimann Systems; Security systems, x-ray inspection, metal scanners
`http://www.heimannsystems.com`

[81] Jochen Kronjäger's High Voltage and X-ray page
`http://www.mathematik.uni-marburg.de/~kronjaeg/hv/`

[82] SPIE Proceedings 1999 Vol. 3577. Paper 3577-08: *Bomb detection using backscattered x rays*

[83] US Customs Today, Issue March 2000: Body Scan system gives passengers a choice
`http://www.customs.ustreas.gov/custoday/mar2000/bodyscan.htm`

[84] Granite Island Group: Technical Surveillance Counter Measures. Video Signal Eavesdropping Threat Tutorial
`http://www.tscm.com/TSCM101video3.html`

[85] Granite Island Group: Vector Signal Analysers
`http://www.tscm.com/tmdevsa.html`

[86] Granite Island Group: Technical Surveillance Counter Measures. Basic Countermeasures Equipment: Video Countermeasures Device
`http://www.tscm.com/mlkVCD.html`

[87] Spy Link International, Inc.: Debugging and Electronic Eavesdropping Countermeasures
`http://www.spy-link.com/catalog/Counter.pdf`

[88] Murray Associates Security Scrapbook, Sun, 06 Jan 2002
`http://www.spybusters.com/SS0201.html`

[89] FRITZ ROBERT. *Spionage, Anti-Terror, IC-Gags, Band 1*. Frech-Verlag, 1978.

[90] Maxim Wideband Transconductance Amplifiers MAX435/MAX436 Datasheet 19-0042, Rev. 1, 4/93

[91] Maxim Application Notes: New Amplifiers Simplify Wideband Techniques `http://dbserv.maxim-ic.com/appnotes.cfm?appnote_number=692`

[92] Marshall Electronics camera V-X0095-PCB `http://www.starkelectronic.com/vx0095.htm`

[93] Samsung KS7214 Timing & Sync. Generator for B/W CCD `http://samsungelectronics.com/semiconductors/System_LSI/Consumer_Multimedia/CCD/KS7214/ks7214.pdf`

[94] Sony timing controllers `http://www.sel.sony.com/semi/ccdarea.html`

[95] OmniVision OV5006 series `http://www.ovt.com/pdfs/OV5016DS.pdf`

[96] OmniVision OV5116 `http://www.ovt.com/pdfs/OV5116LongForm.PDF`

[97] Quasar Electronics CMOS Camera Modules: Cam-2, C-Cam-8, C3186A `http://www.quasarelectronics.com/cmos_cameras.htm`

[98] VLSI Vision Ltd / STMicroelectronics CMOS Image Sensor Products `http://www.vvl.co.uk/products/image_sensors/`

[99] Kameratechnik für Thermographie und Infrarot `http://www.thermografie.de/kamera.htm`

[100] Murray Associates: Thermal Emissions Spectrum Analysis (TESA) `http://www.spybusters.com/infrared.html`

[101] Science & Engineering Associates Security Technology `http://www.seabase.com`

[102] The SEA Technology Store: SpyFinder – Hidden Camera Locator `http://store.yahoo.com/shop-seatech/spyfinder.html`

[103] SpyFinder `http://www.spyfinder.org`

[104] Spy vs. Spy: Device Takes Hidden Cameras Out of Hiding `http://www.techextreme.com/perl/story/14627.html`

[105] Radio waves below 22 kHz – Nature Radio Signals and strange emissions at very low frequency `http://www.vlf.it/localsignals/localsignals.html`

[106] Smart Dust: Autonomous sensing and communication in a cubic millimeter `http://robotics.eecs.berkeley.edu/~pister/SmartDust/`

[107] Webpage with texts, pictures and maps of CCTV installations in Bremen (Germany) and elsewhere
http://www.aktuelle-kamera.org

[108] M.J. Zuckerman, USA Today, November 30, 2000: Chances are, somebodyś watching you
http://www.usatoday.com:80/life/cyber/tech/cti856.htm

[109] Achim Mohné. Surveillance Works 1996 - 2001.
http://www.khm.de/˜achim/